Due Date: December 17, 2007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:	)	
	)	
Inventor: Ronald P. Cocchi et al.	)	Examiner: Syed Zia
	)	
Serial #: 10/085,331	)	Group Art Unit: 2131
	)	
Filed: February 28, 2002	)	Appeal No.: _____
	)	
Title: MULTIPLE NONVOLATILE MEMORIES	)	

BRIEF OF APPELLANTS

MAIL STOP APPEAL BRIEF - PATENTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In accordance with 37 CFR §41.37, Appellants hereby submit the Appellants' Brief on Appeal from the final rejection in the above-identified application, as set forth in the Office Action dated July 17, 2007.

Please charge the amount of $510.00 to cover the required fee for filing this Appeal Brief as set forth under 37 CFR §41.37(a)(2) and 37 CFR §41.20(b)(2) to Deposit Account No. 50-0383 of The DIRECTV Group, Inc., the assignee of the present application. Also, please charge any additional fees or credit any overpayments to Deposit Account No. 50-0383.

I. REAL PARTY IN INTEREST

The real party in interest is The DIRECTV Group, Inc., the assignee of the present application.

II. RELATED APPEALS AND INTERFERENCES

An Appeal Brief was filed with the United States Patent and Trademark Office in related application serial number 10/085,920 on October 1, 2007. No decision has been rendered and no Examiner's Answer has been received at this time.

III. STATUS OF CLAIMS

Claims 1-3, 5-15, 17-27, 29-38, 40-50, and 52-53 are pending in the application.

Claims 1-3, 5-15, 17-27, 29-38, 40-50 and 52-63 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Cohen et al. (5,282,249) and further in view of Kocher (6,289,455).

Claims 1, 12, 24, 35, and 47 stand provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over claims 1, 8, 15, and 22 of Application Serial Number 10/085,920.

Claims 4, 16, 28, 39, and 51 were cancelled.

The rejection of claims 1-3, 5-15, 17-27, 29-38, 40-50 and 52-63 are being appealed herein.

IV. STATUS OF AMENDMENTS

A response under 37 C.F.R. §41.33(a) is being submitted subsequent to the final Office Action, on the same date as this Brief. The response under 37 C.F.R. §41.33(a) includes a Terminal Disclaimer to overcome the obviousness-type double patenting rejections of claims 1, 12, 24, 35, and 47.

Beyond the response under 37 C.F.R. §41.33(a), no amendments to the claims have been made subsequent to the final Office Action.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claims 1, 12, 24, 35, and 47 are generally directed to controlling access to digital services (page 1, lines 19-21). More specifically, digital services are processed in a control center, uplinked to a satellite, and received at a subscriber receiver station where they are processed by a conditional access module (CAM) (page 4, lines 16-23; page 10, line 28-page 11, line 10; FIGs. 1, 5, and 6).

The claims further provide specific limitations relating to the CAM. In this regard, the CAM has a system bus (page 14, line 26, FIG. 6), and a plurality of physically separate and independently controlled nonvolatile memory components (page 14, line 21-page 15, line 2; FIG. 6; page 15, lines 15-28; FIG. 7). Access control to the digital services is distributed among the multiple nonvolatile memory components (page 14, lines 16-20; FIG. 6 and 7 [700] and [702]). In addition, a microprocessor is coupled to each of the nonvolatile memory components (page 15, lines 3-6; page 16, lines 6-8; FIG. 7 [704]) . The microprocessor has various capabilities including the ability to use state information in the memory components to provide desired functionality and enforce a security policy for accessing the digital services (page 16, lines 8-21; FIG. 7). The single microprocessor further controls each of the nonvolatile memory components (page 16, lines 8-21; FIG. 7). Further, the memory components each have separate memory access and control restrictions (page 16, lines 11-12; FIG. 6 and 7).

Accordingly, as set forth above, not only are each of the multiple nonvolatile memory components independently controlled, but they have separate memory access and control restrictions while being controlled by the same microprocessor.

The support for the limitations of the independent claims (and the dependent claims containing means plus function limitations) are set forth in further detail below.

Claim Limitation	Support in Specification.
1. A system for controlling access to digital services comprising:	Page 1, lines 19-21
(a) a control center configured to coordinate and provide digital services;	Page 4, lines 16-23; Page 10, line 28-page 11, line 10; FIGs. 1, 5, and 6
(b) an uplink center configured to receive the digital services from the control center and transmit the digital services to a satellite;	Page 4, lines 16-page 5, line 2; Page 10, line 28-page 11, line 10; FIGs. 1, 5, and 6
(c) the satellite configured to:	Page 4, lines 16-page 5, line 2; Page 10, line 28-page 11, line 10; FIGs. 1, 5, and 6
(i) receive the digital services from the uplink center;	Page 4, lines 16-page 5, line 2; Page 10, line 28-page 11, line 10; FIGs. 1, 5, and 6
(ii) process the digital services; and	Page 4, lines 16-page 5, line 2; Page 10, line 28-page 11, line 10; FIGs. 1, 5, and 6
(iii) transmit the digital services to a subscriber receiver station;	Page 4, lines 16-page 5, line 2; Page 10, line 28-page 11, line 10; FIGs. 1, 5, and 6
(d) the subscriber receiver station configured to:	Page 4, lines 16-page 5, line 13; Page 10, line 28-page 11, line 10; FIGs. 1, 5, and 6
(i) receive the digital services from the satellite;	Page 4, lines 16-page 5, line 13; Page 10, line 28-page 11, line 10; FIGs. 1, 5, and 6
(ii) control access to the digital services through an integrated receiver/decoder (IRD);	Page 4, lines 16-page 5, line 13; Page 10, line 28-page 11, line 10; FIGs. 1, 5, and 6
(e) a conditional access module (CAM) communicatively coupled to the (IRD), wherein the CAM comprises:	Page 4, lines 16-page 5, line 13; Page 10, line 28-page 11, line 10; FIGs. 1, 5, and 6
(i) a system bus;	Page 14, line 26; FIG. 6

(ii) a plurality of physically separate and independently controlled nonvolatile memory components, wherein access control to the digital services is distributed among the nonvolatile memory components wherein separate and independent attacks must be conducted on each nonvolatile memory component to gain unauthorized access to the digital services; and	Page 14, line 16-page 15, line 2; FIG. 6; Page 15, lines 1-28; page 16, lines 17-21; FIG. 7 [700] and [702]
(iii) a microprocessor communicatively coupled to the nonvolatile memory components, wherein the microprocessor is configured to use state information in the nonvolatile memory components to provide desired functionality and enforce one or more security policies for accessing the digital services, and wherein the microprocessor controls each of the plurality of nonvolatile memory components and each nonvolatile memory component has separate memory access and control restrictions.	Page 2, lines 17-21; Page 14, line 21-page 15, line 6; page 16, lines 6-21; FIG. 6 and FIG. 7 [704]
12. A method of controlling unauthorized access to digital services	Page 1, lines 19-21

comprising:	
distributing access to digital services among a plurality of physically separate and independently controlled nonvolatile memory components on a system bus wherein separate and independent attacks must be conducted on each of the nonvolatile memory components to gain unauthorized access to the digital services; and	Page 14, line 16-page 15, line 2; FIG. 6; Page 15, lines 1-28; page 16, lines 17-21; FIG. 7 [700] and [702]
communicatively coupling the plurality of nonvolatile memory components to a microprocessor, wherein the microprocessor is configured to use state information in the nonvolatile memory components to provide desired functionality and enforce one or more security policies for accessing the digital services, and wherein the microprocessor controls each of the plurality of nonvolatile memory components and each nonvolatile memory component has separate memory access and control restrictions.	Page 2, lines 17-21; Page 14, line 21-page 15, line 6; page 16, lines 6-21; FIG. 6 and FIG. 7 [704]
24. A method of accessing digital services comprising:	Page 1, lines 19-21
storing state information in a plurality of nonvolatile memory components, wherein the plurality of nonvolatile memory components are physically separate and independently controlled, wherein separate and independent attacks must be conducted on each of the nonvolatile	Page 14, line 16-page 15, line 2; FIG. 6; Page 15, lines 1-28; page 16, lines 17-21; FIG. 7 [700] and [702]

memory components to gain unauthorized access to the digital services;	
accessing digital services using the nonvolatile memory components wherein the state information is used to provide desired functionality and enforce one or more security policies for accessing the digital services, and wherein the microprocessor controls each of the plurality of nonvolatile memory components and each nonvolatile memory component has separate memory access and control restrictions.	Page 2, lines 17-21; Page 14, line 21-page 15, line 6; page 16, lines 6-21; FIG. 6 and FIG. 7 [704]
35. A conditional access module (CAM), comprising:	Page 4, lines 16-page 5, line 13; Page 10, line 28-page 11, line 10; FIGs. 1, 5, and 6
a system bus;	Page 14, line 26; FIG. 6
a plurality of physically separate and independently controlled nonvolatile memory components, wherein access control to digital services is distributed among the nonvolatile memory components, and wherein separate and independent attacks must be conducted on each of the nonvolatile memory components to gain unauthorized access to the digital services; and	Page 14, line 16-page 15, line 2; FIG. 6; Page 15, lines 1-28; page 16, lines 17-21; FIG. 7 [700] and [702]
a microprocessor communicatively coupled to the nonvolatile memory components, wherein the microprocessor is configured to use state information in the nonvolatile memory components to provide desired functionality and enforce one or more security policies for	Page 2, lines 17-21; Page 14, line 21-page 15, line 6; page 16, lines 6-21; FIG. 6 and FIG. 7 [704]

accessing the digital services, and wherein the microprocessor controls each of the plurality of nonvolatile memory components and each nonvolatile memory component has separate memory access and control restrictions.	
47. An article of manufacture for preventing unauthorized access to digital services comprising:	Abstract, Page 24, lines 1-8; Page 1, lines 19-21
means for distributing access control to digital services among a plurality of physically separate and independently controlled nonvolatile memory components on a system bus, and wherein separate and independent attacks must be conducted on each of the nonvolatile memory components to gain unauthorized access to the digital services; and	Means+Function Limitation; Structure, material, or acts for the claimed function are set forth on page 14, line 16-page 15, line 2; FIG. 6; Page 15, lines 1-28; page 16, lines 17-21; FIG. 7 [700] and [702];
means for communicatively coupling the plurality of nonvolatile memory components to a microprocessor, wherein the microprocessor is configured to use state information in the nonvolatile memory components to provide desired functionality and enforce one or more security policies for accessing the digital services, and wherein the microprocessor controls each of the plurality of nonvolatile memory components and each nonvolatile memory component has separate memory access and control restrictions.	Means+Function Limitation; Structure, material, or acts for the claimed function are set forth on page 2, lines 17-21; Page 14, line 21-page 15, line 6; page 16, lines 6-21; FIG. 6 and FIG. 7 [704]

55. The article of manufacture of claim 53, further comprising means for sharing programming control between the plurality of nonvolatile memory components.	Means+Function Limitation; Structure, material, or acts for the claimed function are set forth on page 15, lines 7-13; FIGs. 5 and 6.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether claims 1-3, 5-15, 17-27, 29-38, 40-50 and 52-63 are unpatentable under 35 U.S.C. § 103(a) as being rendered obvious by Cohen et al., U.S. Patent No. 5,282,249 (Cohen) and Kocher, U.S. Patent No. 6,289,455 (Kocher).

VII. ARGUMENT

Claims 1-3, 5-15, 17-27, 29-38, 40-50 and 52-63 are Patentable under 35 U.S.C. § 103(a) over Cohen et al., U.S. Patent No. 5,282,249 (Cohen) and Kocher, U.S. Patent No. 6,289,455 (Kocher).

A. Claims 1, 12, 24, 35 and 47

Appellant traverses the rejections as set forth in the final Office Action for one or more of the following reasons:

(1) Neither Cohen nor Kocher teach, disclose or suggest a single microprocessor that controls multiple nonvolatile memory components that are physically separate and independently controlled; and

(2) Neither Cohen nor Kocher teach, disclose or suggest a single microprocessor that controls multiple nonvolatile memory components with separate memory access control restrictions.

The Office Action admits Cohen's lack of teaching of multiple nonvolatile memory components as claimed. To teach these elements of the claims, the Office Action relies on Kocher col. 21, line 13 to col. 22 line 25 and col. 24, line 10 to line 30. Appellants respectfully disagree with and traverse such rejections. Namely, these portions of Kocher completely fail to describe multiple nonvolatile memory components organized in the manner claimed. Instead, Kocher merely describes multiple microprocessors that each may have its own RAM, ROM, and EEPROM (see

col. 21, lines 34-40). However, the ability for a single microprocessor to independently control separate nonvolatile memory components is not taught or disclosed, explicitly or implicitly, in Kocher. The use of multiple nonvolatile memory components as claimed provides significant advantages over the prior art including Kocher. Paragraph [0062] of the application as filed describes some of such advantages:

> **[0062]** FIG. 6 illustrates the architecture of a CAM 512 in accordance with one or more embodiments of the invention. The CAM 512 contains a microprocessor 602, volatile memory components 604 (e.g., random access memory [RAM]), a plurality of nonvolatile memory components 606 (e.g., electrical erasable programmable read only memory [EEPROM], erasable programmable read only memory [EPROM], or batter packed RAM), and a system input/output module 608, all of which are communicatively coupled to a system bus 610. As illustrated, a plurality of nonvolatile memory components 606 are utilized. Using this approach, each nonvolatile memory component 606 has separate memory access control restrictions and may implement entirely unique memory access control logic. This forces an intruder to embark on multiple separate attacks to compromise each memory component 606.

As can be seen, such an approach forces an intruder to attempt multiple separate attacks in order to access each separate memory component and gain access to the digital services. However, Kocher does not even remotely allude to such a benefit or capability. Instead, Kocher merely describes two microprocessors – one serves as an interface control processor (ICP) that communicates with a second processor that is a cryptofirewall that controls access to a protected memory (see col. 7, lines 54-60 and col. 21, lines 34-54). However, such a teaching completely and totally fails to describe or suggest a single microprocessor that access multiple nonvolatile memory components that are not in protected memory.

Appellants further note that claims 3, 24, 37, and 49 provide a limitation for a custom logic block that is further described in copending patent applications (see argument below). It is noted that the custom logic block controls access to memory. However, the multiple nonvolatile memories of the present invention are not controlled by the custom logic block. FIG. 6 of the present invention illustrates the multiple nonvolatile memory components of the system as claimed. There are clearly significant, distinguishable, and nonobvious differences from the system of FIG. 6 as claimed and Kocher (and/or the combination of Kocher with Cohen).

In response to the above, the final Office Action provides that Kocher teaches a system and method that relates to a number of selectable and portable executing devices, each being operatively associated with any one receiving descrambler and each executing identical operations to generate a

seed for use by the associated receiving descrambler to enable the receiving descrambler to descramble the broadcast. The final Office Action relies on Kocher Fig. 1-2, col. 4, line 12-66, col 21, line 2-col. 22, line 25. Further the Action provides:

> In particular, fixed data and code are stored in ROM, temporary data (and possibly code) are stored in RAM, and additional code and/or data are stored in EEPROM which can be modified by processor. Also attached to bus is CryptoFirewall, a specialized cryptographic processing unit which regulates and cryptographically modifies data written to or read from protected memory (Fig. 2, col. 9, line 29 to line 59).

Appellants note that RAM is not nonvolatile memory. Further, the CryptoFirewall contains a processing unit itself and merely modifies data written to or read from protected memory (see col. 9, lines 37-41).

The claims provide that access control to the digital services is distributed among the multiple nonvolatile memory components. Further, separate and independent attacks must be conducted on each of the nonvolatile memory components to gain unauthorized access to the digital services. Thus, rather than being able to attack one nonvolatile memory unit and gaining access to all of the digital services, the present invention provides that all of the nonvolatile memory components must be accessed to gain access to the digital services. Merely accessing one component is insufficient. Appellants again direct the attention of the patent office to paragraphs [0059]-[0068] of the originally filed specification. For example, paragraph [0061] provides as follows:

> **[0061]** To avoid this method of attack, access to the nonvolatile memory components is distributed among several physically separate and independently controlled nonvolatile memory components. Using this approach, it may not be possible to compromise one nonvolatile memory component and march through all memory address locations that reside other memory components. Only the attacked memory component is compromised.

Similarly, paragraph [0065] provides as follows:

> **[0065]** There are many advantages to using a plurality of nonvolatile memory components 606 in a CAM 512. For example, the nonvolatile memory components 606 have physically separate address spaces and physical locations on the die. Further, each nonvolatile memory component 606 would have to be attacked and compromised separately. Separate memory control units can be implemented allowing each control unit to be uniquely customized and tailored to the specific memory module 606 being protected. This design requires each nonvolatile memory component 606 to be attacked separately and individually. Therefore, the entire chip can withstand substantial external attack through the system I/O module 608. Accordingly, the use of such a plurality of nonvolatile memory components enables the protection of video, audio, broadband, and data/digital services reception.

Lastly, paragraph [0068] provides as follows:

> **[0004]** At step 706, digital services are accessed using the nonvolatile memory components 606 to provide desired functionality and enforce security policies for the access. Using the identified configuration with a plurality of nonvolatile memory components 606, if unauthorized access is attempted, separate and independent attacks must be conducted on each nonvolatile memory component 606.

As can be seen, the invention as claimed provides more than merely reciting multiple nonvolatile memory components. Instead, the multiple components control access to the digital services and provide for a more secure environment. Further, the access control is distributed across the multiple components. Thus, even if one component were compromised, the access to the digital services would not be compromised without also gaining access to the remaining components. The various teachings of Kocher do not even remotely refer to or resemble such an architecture or secure system as claimed. Further, the final Office Action fails to describe how Kocher teaches such explicit and detailed claim limitations.

Again, while Kocher teaches (in FIG. 1 and 2), a memory connected to a microprocessor (Fig. 1), and ROM245 and EEPROM 255 connected to a bus 240 (Fig. 2), neither Kocher Fig. 1 nor Kocher Fig. 2 depict the limitations of the claims. Further, Kocher's specification also fails to describe the claim limitations. What is notoriously lacking from Kocher is any description of distributing access control to digital services across multiple nonvolatile memory components that have to be separately attacked in order to gain access to the digital services (as claimed). Instead, Kocher merely refers to the use of ROM 245 and EEPROM 255 in addition to the use of protected memory 265 via cryptofirewall 260. Such a use of the cryptofirewall 260 is irrelevant to the present claims since a separate microprocessor exists within the cryptofirewall as described above (while the present claims require a single microprocessor). Further, the other components do not control access to digital services. Thus, Kocher does not and cannot teach the invention as claimed.

In response to the above arguments, the prior Office Action merely provides that a cryptographic unit transforms data from the microprocessor and uses memory contents and the transformation result is utilized to decode digital content. The Action continues and provides that the CRU includes an interface control processor (ICP) that is responsible for communication with a playback device and includes several types of memory connected to the ICP via bus. The Action states that in particular, fixed data and code are stored in ROM, temporary data is stored in RAM,

and additional code and/or data is stored in EEPROM that can be modified by the processor. Further, the Action provides that a cryptofirewall and cryptographic processing unit are attached to the bus and are used to regulate and cryptographically modify data written to or read from protected memory.

However, what is missing from such a description is a plurality of independently controlled nonvolatile memory components wherein access control to the digital services is distributed among the components. Firstly, RAM is irrelevant since it is not nonvolatile memory. Secondly, the access control to the digital services is NOT distributed across Kocher's ROM and EEPROM.

The claim limitations relating to distribution of access control are further set expressly in the claims that provide that separate and independent attacks must be conducted on each nonvolatile memory component to gain access to the digital services. Further, state information in the nonvolatile memory components is used by the microprocessor to enforce security policies for accessing the digital services. In addition, the single microprocessor controls each of the nonvolatile memory components via separate memory access and control restrictions. Again, Kocher fails to provide or even remotely allude to such a teaching. Instead, Kocher describes for storing fixed data and code in ROM and additional code and/or data in EEPROM. However, there is no mention or description that such code and/or data is part of an access control system that has been distributed across the ROM and EEPROM. Nor is there any mention or description, explicit or implicit, that to gain unauthorized access to the digital services, separate and independent attacks must be conducted on both the ROM and EEPROM.

Instead of even alluding to the claimed limitations, Kocher provides for utilizing two microprocessors that each have their own RAM, ROM and EEPROM (see col. 21, lines 35-39). In this regard, one microprocessor serves as the ICP and communicates with a second microprocessor which is the cryptofirewall. However, contrary to that set forth in the claims, Kocher has different memories for each microprocessor. Further and more importantly, the access control to the digital services is not distributed across multiple memories that are controlled by a single microprocessor (as claimed).

In view of the above, it is noted that the Office Action ignores the claim limitations relating to the distribution of access control. The Office Action further ignores the explicit claim limitations

providing that separate and independent attacks must be conducted on each nonvolatile component to gain unauthorized access. Under MPEP §2142 and 2143.03 "To establish *prima facie* obviousness of a claimed invention, all the claim limitations must be taught or suggested by the prior art. *In re Royka*, 490 F.2d 981, 180 USPQ 580 (CCPA 1974). "All words in a claim must be considered in judging the patentability of that claim against the prior art." *In re Wilson*, 424 F.2d 1382, 1385, 165 USPQ 494, 496 (CCPA 1970)." The Office Action has failed to address all of the claim limitations or has merely summarily rejected them without stating where either reference teaches such a limitation.

The Office Action groups together all of the limitations relating to the nonvolatile memory components into one paragraph and summarily recites Kocher, col. 10, lines 5 to 47, col. 5, line 55 to col. 6, line 3, and col. 24, line 10 to line 30. Col. 10, lines 5-47 merely describe a protected memory having EEPROM and the use of different keys. However, the distribution of access control is neither described or alluded to. Col. 5, line 55 to col. 6, line 3 merely describes a summary of Kocher's security system that includes a microprocessor, a memory, a cryptographic unit connected between the microprocessor and the memory that protects the memory, and a device key accessible by the cryptographic unit and inaccessible by the microprocessor such that the cryptographic unit uses the contents of the memory to transform a data value received from the microprocessor that is required to decode the digital content. However, once again, such a description fails to describe the distribution of access control across multiple nonvolatile memory components wherein separate and independent attacks of each component are required to gain unauthorized access to the digital services (as claimed).

Col. 24, lines 10-30 describe how a physical invasive attack can provide the ability to read from and/or write to the protected memory. The text further describes that such reading/writing provides no particular value, since the keys stored in the protected memory are not useful without the algorithms that are implemented in the cryptographic unit. The text then describes that a proper functioning cryptofirewall is still required to process the values from the protected memory into content decryption keys. The text concludes by stating: "AS A RESULT, THE ATTACKER'S WORK MODIFYING ONE CHIP CAN YIELD ONE FULLY-FUNCTIONAL PIRATE DEVICE, BUT SHOULD NOT LEAD TO A GENERAL ATTACK THAT CAN BE

MARKETED ON A WIDE SCALE". As can be seen, rather than preventing access to digital services, Kocher explicitly teaches that a pirate device can be created merely by accessing the protected memory. Such a teaching would actually serve to teach away from the present invention since such a device would not require independent and separate attacks of each nonvolatile memory component. In addition, such a teaching completely and wholly fails to describe distributing access control across multiple nonvolatile memory components that are controlled by a single microprocessor yet has separate memory access and control restrictions. Again, Kocher fails to describe or suggest the explicit and detail claim limitations that are set forth in the present claims. Instead, the mere interaction between a CRU and microrprocessor are described without any reference or description to the limitations set forth in the claims and described herein.

In addition to the above, Appellants note that the other cited references also fails to cure Kocher's deficiencies.

Moreover, the various elements of Appellants' claimed invention together provide operational advantages over Cohen and Kocher. In addition, Appellants' invention solves problems not recognized by Cohen and Kocher.

In response to the above arguments, the final Office Action essentially repeats the prior rejections. The final Action again repeats that attached to the bus is a cryptofirewall, that is a specialized cryptographic processing unit which regulates and cryptographically modifies data written to or read from protected memory. As described in detail below dependent claims 59-63 provide for protected memory and clearly distinguish such memory from the other multiple nonvolatile memory components that are controlled by a single microprocessor. In this regard, Kocher explicitly recites multiple processors rather than the single microprocessor that controls multiple nonvolatile memory components all of which must be accessed independently in order to gain access to digital services as claimed. Regardless of whether Kocher recites the ability to prevent unauthorized access to digital services, the present claims provide for more than merely preventing access - they explicitly recite specific limitations that are used to prevent such access. Namely, the single microprocessor accesses multiple nonvolatile memory components:

"a plurality of physically separate and independently controlled nonvolatile memory components, wherein access control to the digital services is distributed among the nonvolatile

memory components wherein separate and independent attacks must be conducted on each nonvolatile memory component to gain unauthorized access to the digital services;"

Again, such claim limitations are not even remotely hinted at or suggested in either the text or Figures of Kocher or Cohen.

In view of the above, Appellants respectfully request reversal of the rejections.

B. Dependent claims 3, 14, 37, 49

Appellants further note that claims 3, 14, 37, and 49 provide a limitation for a custom logic block that is further described in copending patent applications. It is noted that the custom logic block controls access to memory. However, the multiple nonvolatile memories of the present invention are not controlled by the custom logic block. FIG. 6 of the present invention illustrates the multiple nonvolatile memory components of the system as claimed. There are clearly significant, distinguishable, and nonobvious differences from the system of FIG. 6 as claimed and Kocher (and/or the combination of Kocher with Cohen).

C. Dependent claims 5, 17, 29, 40, and 52

These dependent claims provide that each nonvolatile memory component implements an entirely unique memory access control logic. In rejecting these claims, the final Office Action merely refers to Kocher col. 23, line 36 to line 48. Such text provides:

> Under the architecture outlined in FIG. 2, the system remains robust even if the ICP and its RAM, ROM, and EEPROM are compromised. This is an extremely important feature of the present design, since these components of a chip are particularly vulnerable to both invasive and non-invasive attacks. The CryptoFirewall controls the addition of rights keys to the protected memory and thereby prevents information obtained from one CRU from providing attackers with the ability to add rights keys to other CRUs without breaking the cryptography or performing an invasive attack. Even if rights keys are compromised, attackers cannot insert them behind the CryptoFirewall.

As can be seen, such text does not even remotely hint at each nonvolatile memory component implementing unique memory access control logic. Instead, such text merely describes the use of rights keys in protected memory (i.e., memory behind the CryptoFirewall). Further, the remaining portions of Kocher (and Cohen) also fail to describe these claim limitations.

In view of the above, Appellants respectfully request reversal of the rejections.

D. Dependent claims 6, 18, 30, 41, and 53 Are Not Separately Argued

E. Dependent claims 7, 19, 42, and 54 Are Not Separately Argued

F. Dependent claims 8, 20, 31, 43, and 55 Are Not Separately Argued

G. Dependent claims 9, 21, 32, 44, and 56 Are Not Separately Argued

H. Dependent claims 10, 22, 33, 45, and 57

These dependent claims provide that the plurality of nonvolatile memory components employ a single contiguous address range.

In rejecting these claims, the final Office Action merely recites Kocher col. 27, lines 25-39 which provides:

> Some steps, such as address verification by the CryptoFirewall, are recommended but may be omitted as they are not always essential. Steps can also be substituted with other operations that are functionally similar. For example, address verification can be performed by forcing invalid addresses to valid values (e.g., by setting or clearing bits in the address to ensure that the address is in a proper range and aligned appropriately). Many steps can also be reordered. For example, the chip-specific portion of the computation described with respect to FIG. 7 can be XORed with the BATCH_KEY computation result instead of with the BATCH_KEY computation input. Many other such simple variants will be evident to one of ordinary skill in the art.

As can clearly be seen, such text describes that the CryptoFirewall can perform address verification by forcing invalid addresses to valid values. However, what is missing from such a description is a teaching or suggestion that multiple components use the same contiguous address range. The ability to force invalid addresses into valid addresses by setting or clearing bits in an address is not even remotely similar to providing for the use of a single contiguous address range as claimed.

Further, the use of such an address range in the present application is possible because the components are controlled and programmed by the same microprocessor. Such capabilities are lacking from Kocher (as described above).

In view of the above, Appellants respectfully request reversal of the rejections.

I. Dependent claims 11, 23, 34, 46, and 58 Are Not Separately Argued

J. Dependent claims 15, 26, and 50 Are Not Separately Argued

K. Dependent claim 27 is Not Separately Argued

L. Dependent claims 59-63

Dependent claims 59-63 provide that at least one of the plurality of physically separate and independently controlled nonvolatile memory components is protected from modification such that the protected nonvolatile memory component is read only, and access to the protected nonvolatile memory component is isolated. Further, these claims provide that a microprocessor's unprotected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same. Such a teaching and use of the same physical and logical address ranges across multiple different nonvolatile memory components is neither taught nor suggested by any of the cited references.

In rejecting these claims, the Office Action relies on Kocher Fig. 2, col. 9, lines 29-59 and col. 27, lines 25-39. A close examination of such text (and the remainder of Kocher) clearly reveals a lack of such a teaching. In this regard, Kocher explicitly recites multiple processors rather than the single microprocessor that controls multiple nonvolatile memory components - all of which must be accessed independently in order to gain access to digital services as claimed. Regardless of whether Kocher recites the ability to prevent unauthorized access to digital services, the present claims provide for more than merely preventing access - they explicitly recite specific limitations that are used to prevent such access. Namely, the single microprocessor accesses multiple nonvolatile memory components:

"a plurality of physically separate and independently controlled nonvolatile memory components, wherein access control to the digital services is distributed among the nonvolatile memory components wherein separate and independent attacks must be conducted on each nonvolatile memory component to gain unauthorized access to the digital services;"

Again, such claim limitations are not even remotely hinted at or suggested in either the text or Figures of Kocher or Cohen.

In view of the above, Appellants respectfully request reversal of the rejections.

VIII. CONCLUSION

In light of the above arguments, Appellants respectfully submit that the cited references do not anticipate nor render obvious the claimed invention. More specifically, Appellants' claims recite novel physical features which patentably distinguish over any and all references under 35 U.S.C. §§ 102 and 103. As a result, a decision by the Board of Patent Appeals and Interferences reversing the Examiner and directing allowance of the pending claims in the subject application is respectfully solicited.

Respectfully submitted,

Attorneys for Appellant(s)

Date: December 17, 2007

By: /Jason S. Feldmar/
Name: Jason S. Feldmar
Reg. No.: 39,187

JSF/sjm

G&C 109.68-US-01

CLAIMS APPENDIX

1. (PREVIOUSLY PRESENTED) A system for controlling access to digital services comprising:

(a) a control center configured to coordinate and provide digital services;

(b) an uplink center configured to receive the digital services from the control center and transmit the digital services to a satellite;

(c) the satellite configured to:

(i) receive the digital services from the uplink center;

(ii) process the digital services; and

(iii) transmit the digital services to a subscriber receiver station;

(d) the subscriber receiver station configured to:

(i) receive the digital services from the satellite;

(ii) control access to the digital services through an integrated receiver/decoder (IRD);

(e) a conditional access module (CAM) communicatively coupled to the (IRD), wherein the CAM comprises:

(i) a system bus;

(ii) a plurality of physically separate and independently controlled nonvolatile memory components, wherein access control to the digital services is distributed among the nonvolatile memory components wherein separate and independent attacks must be conducted on each nonvolatile memory component to gain unauthorized access to the digital services; and

(iii) a microprocessor communicatively coupled to the nonvolatile memory components, wherein the microprocessor is configured to use state information in the nonvolatile memory components to provide desired functionality and enforce one or more security policies for accessing the digital services, and wherein the microprocessor controls each of the plurality of nonvolatile memory components and each nonvolatile memory component has separate memory access and control restrictions.

2. (ORIGINAL) The system of claim 1, wherein the conditional access module is a smart card.

3. (ORIGINAL) The system of claim 2, wherein the smart card further comprises:

a volatile memory component;

a custom logic block; and

a system input/output module.

4. (CANCELLED)

5. (ORIGINAL) The system of claim 1, wherein each nonvolatile memory component implements an entirely unique memory access control logic.

6. (ORIGINAL) The system of claim 1, wherein the plurality of nonvolatile memory components reside on a single chip.

7. (ORIGINAL) The system of claim 6, wherein a charge pump is shared between the plurality of nonvolatile memory components.

8. (ORIGINAL) The system of claim 6, wherein programming control is shared between the plurality of nonvolatile memory components.

9. (ORIGINAL) The system of claim 1, wherein the plurality of nonvolatile memory components employ separate and unique address ranges.

10. (ORIGINAL) The system of claim 1, wherein the plurality of nonvolatile memory components employ a single contiguous address range.

11. (ORIGINAL) The system of claim 1, wherein separate access control units satisfy a functional requirement of each nonvolatile memory component.

12. (PREVIOUSLY PRESENTED) A method of controlling unauthorized access to digital services comprising:

distributing access to digital services among a plurality of physically separate and independently controlled nonvolatile memory components on a system bus wherein separate and independent attacks must be conducted on each of the nonvolatile memory components to gain unauthorized access to the digital services; and

communicatively coupling the plurality of nonvolatile memory components to a microprocessor, wherein the microprocessor is configured to use state information in the nonvolatile memory components to provide desired functionality and enforce one or more security policies for accessing the digital services, and wherein the microprocessor controls each of the plurality of nonvolatile memory components and each nonvolatile memory component has separate memory access and control restrictions.

13. (ORIGINAL) The method of claim 12, wherein the plurality of nonvolatile memory components are contained within a security component known as a smart card.

14. (ORIGINAL) The method of claim 13, wherein the smart card further comprises:

a volatile memory component;

a custom logic block; and

a system input/output module.

15. (ORIGINAL) The method of claim 13, wherein the smart card is utilized in an integrated receiver/decoder (IRD).

16. (CANCELLED)

17. (ORIGINAL) The method of claim 12, wherein each nonvolatile memory component implements an entirely unique memory access control logic.

18. (ORIGINAL) The method of claim 12, wherein the plurality of nonvolatile memory components reside on a single chip.

19. (ORIGINAL) The method of claim 18, wherein a charge pump is shared between the plurality of nonvolatile memory components.

20. (ORIGINAL) The method of claim 18, wherein programming control is shared between the plurality of nonvolatile memory components.

21. (ORIGINAL) The method of claim 12, wherein the plurality of nonvolatile memory components employ separate and unique address ranges.

22. (ORIGINAL) The method of claim 12, wherein the plurality of nonvolatile memory components employ a single contiguous address range.

23. (ORIGINAL) The method of claim 12, wherein separate access control units satisfy a functional requirement of each nonvolatile memory component.

24. (PREVIOUSLY PRESENTED) A method of accessing digital services comprising:

storing state information in a plurality of nonvolatile memory components, wherein the plurality of nonvolatile memory components are physically separate and independently controlled,

wherein separate and independent attacks must be conducted on each of the nonvolatile memory components to gain unauthorized access to the digital services;

accessing digital services using the nonvolatile memory components wherein the state information is used to provide desired functionality and enforce one or more security policies for accessing the digital services, and wherein the microprocessor controls each of the plurality of nonvolatile memory components and each nonvolatile memory component has separate memory access and control restrictions.

25. (ORIGINAL) The method of claim 24, wherein the plurality of nonvolatile memory components are contained within a security component known as a smart card.

26. (ORIGINAL) The method of claim 25, wherein the smart card is utilized in an integrated receiver/decoder (IRD).

27. (ORIGINAL) The method of claim 24, wherein a single microprocessor controls the nonvolatile memory components.

28. (CANCELLED)

29. (ORIGINAL) The method of claim 24, wherein each nonvolatile memory component implements an entirely unique memory access control logic.

30. (ORIGINAL) The method of claim 24, wherein the plurality of nonvolatile memory components reside on a single chip.

31. (ORIGINAL) The method of claim 30, wherein programming control is shared between the plurality of nonvolatile memory components.

32. (ORIGINAL) The method of claim 24, wherein the plurality of nonvolatile memory components employ separate and unique address ranges.

33. (ORIGINAL) The method of claim 24, wherein the plurality of nonvolatile memory components employ a single contiguous address range.

34. (ORIGINAL) The method of claim 24, wherein separate access control units satisfy a functional requirement of each nonvolatile memory component.

35. (PREVIOUSLY PRESENTED) A conditional access module (CAM), comprising:

a system bus;

a plurality of physically separate and independently controlled nonvolatile memory components, wherein access control to digital services is distributed among the nonvolatile memory components, and wherein separate and independent attacks must be conducted on each of the nonvolatile memory components to gain unauthorized access to the digital services; and

a microprocessor communicatively coupled to the nonvolatile memory components, wherein the microprocessor is configured to use state information in the nonvolatile memory components to provide desired functionality and enforce one or more security policies for accessing the digital services, and wherein the microprocessor controls each of the plurality of nonvolatile memory components and each nonvolatile memory component has separate memory access and control restrictions.

36. (ORIGINAL) The CAM of claim 35, wherein the conditional access module is a smart card.

37. (ORIGINAL) The CAM of claim 36, wherein the smart card further comprises:

a volatile memory component;

a custom logic block; and

a system input/output module.

38. (ORIGINAL) The CAM of claim 36, wherein the smart card is utilized in an integrated receiver/decoder (IRD).

39. (CANCELLED)

40. (ORIGINAL) The CAM of claim 35, wherein each nonvolatile memory component implements an entirely unique memory access control logic.

41. (ORIGINAL) The CAM of claim 35, wherein the plurality of nonvolatile memory components reside on a single chip.

42. (ORIGINAL) The CAM of claim 41, wherein a charge pump is shared between the plurality of nonvolatile memory components.

43. (ORIGINAL) The CAM of claim 41, wherein programming control is shared between the plurality of nonvolatile memory components.

44. (ORIGINAL) The CAM of claim 35, wherein the plurality of nonvolatile memory components employ separate and unique address ranges.

45. (ORIGINAL) The CAM of claim 35, wherein the plurality of nonvolatile memory components employ a single contiguous address range.

46. (ORIGINAL) The CAM of claim 35, wherein separate access control units satisfy a functional requirement of each nonvolatile memory component.

47. (PREVIOUSLY PRESENTED) An article of manufacture for preventing unauthorized access to digital services comprising:

means for distributing access control to digital services among a plurality of physically separate and independently controlled nonvolatile memory components on a system bus, and wherein separate and independent attacks must be conducted on each of the nonvolatile memory components to gain unauthorized access to the digital services; and

means for communicatively coupling the plurality of nonvolatile memory components to a microprocessor, wherein the microprocessor is configured to use state information in the nonvolatile memory components to provide desired functionality and enforce one or more security policies for accessing the digital services, and wherein the microprocessor controls each of the plurality of nonvolatile memory components and each nonvolatile memory component has separate memory access and control restrictions.

48. (ORIGINAL) The article of manufacture of claim 47, wherein the plurality of nonvolatile memory components are contained within a security component known as a smart card.

49. (ORIGINAL) The article of manufacture of claim 48, wherein the smart card further comprises:

a volatile memory component;

a custom logic block; and

a system input/output module.

50. (ORIGINAL) The article of manufacture of claim 48, wherein the smart card is utilized in an integrated receiver/decoder (IRD).

51. (CANCELLED)

52. (ORIGINAL) The article of manufacture of claim 47, wherein each nonvolatile memory component implements an entirely unique memory access control logic.

53. (ORIGINAL) The article of manufacture of claim 47, wherein the plurality of nonvolatile memory components reside on a single chip.

54. (ORIGINAL) The article of manufacture of claim 53, wherein a charge pump is shared between the plurality of nonvolatile memory components.

55. (ORIGINAL) The article of manufacture of claim 53, further comprising means for sharing programming control between the plurality of nonvolatile memory components.

56. (ORIGINAL) The article of manufacture of claim 47, wherein the plurality of nonvolatile memory components employ separate and unique address ranges.

57. (ORIGINAL) The article of manufacture of claim 47, wherein the plurality of nonvolatile memory components employ a single contiguous address range.

58. (ORIGINAL) The article of manufacture of claim 47, wherein separate access control units satisfy a functional requirement of each nonvolatile memory component.

59. (PREVIOUSLY PRESENTED) The system of claim 1, wherein:

(a) at least one of the plurality of physically separate and independently controlled nonvolatile memory components is protected, wherein:

(i) the protected nonvolatile memory component is protected from modification such that the protected nonvolatile memory component is read only; and

(ii) access to the protected nonvolatile memory component is isolated;

(b) the CAM further comprises a microprocessor's unprotected nonvolatile memory component wherein the microprocessor's unprotected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same.

60. (PREVIOUSLY PRESENTED) The method of claim 12, wherein:

(a) at least one of the plurality of physically separate and independently controlled nonvolatile memory components is protected, wherein:

(i) the protected nonvolatile memory component is protected from modification such that the protected nonvolatile memory component is read only; and

(ii) access to the protected nonvolatile memory component is isolated;

(b) a microprocessor's unprotected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same.

61. (PREVIOUSLY PRESENTED) The method of claim 24, wherein:

(a) at least one of the plurality of physically separate and independently controlled nonvolatile memory components is protected, wherein:

(i) the protected nonvolatile memory component is protected from modification such that the protected nonvolatile memory component is read only; and

(ii) access to the protected nonvolatile memory component is isolated;

(b) a microprocessor's unprotected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same.

62. (PREVIOUSLY PRESENTED) The CAM of claim 35, wherein:

(a) at least one of the plurality of physically separate and independently controlled nonvolatile memory components is protected, wherein:

(i) the protected nonvolatile memory component is protected from modification such that the protected nonvolatile memory component is read only; and

(ii) access to the protected nonvolatile memory component is isolated;

(b) the CAM further comprises a microprocessor's unprotected nonvolatile memory component wherein the microprocessor's unprotected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same.

63. (PREVIOUSLY PRESENTED) The article of manufacture of claim 47, wherein:

(a) at least one of the plurality of physically separate and independently controlled nonvolatile memory components is protected, wherein:

(i) the protected nonvolatile memory component is protected from modification such that the protected nonvolatile memory component is read only; and

(ii) access to the protected nonvolatile memory component is isolated;

(b) a microprocessor's unprotected nonvolatile memory component and the protected nonvolatile memory component use physical and logical address ranges that are the same.

EVIDENCE APPENDIX

None.

RELATED PROCEEDINGS APPENDIX

None.